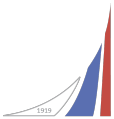
Об одном подходе к построению режимов работы блочных шифров для защиты информации на системных носителях с блочно-ориентированной структурой

Коренева А.М.[1,2], Фирсов Г.В.[1,3]

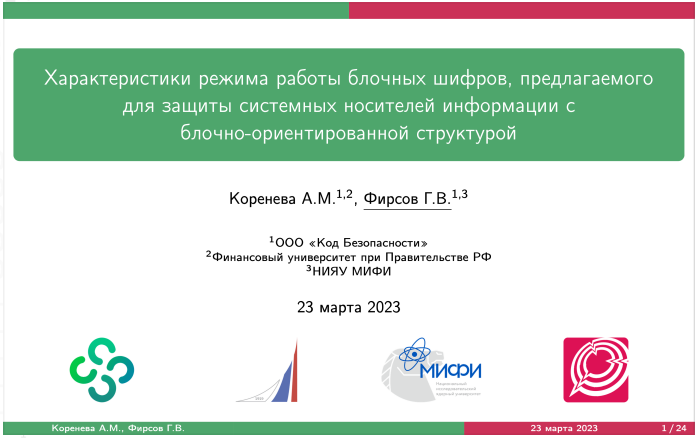
[1]ООО «Код Безопасности»
[2]Финансовый университет при Правительстве РФ
[3]НИЯУ МИФИ

19 марта 2025



Два года назад на РусКрипто'2023...

Режим XEH


Характеристики режима работы блочных шифров, предлагаемого для защиты системных носителей информации с блочно-ориентированной структурой

Коренева А.М.[1,2], Фирсов Г.В.[1,3]

[1]ООО «Код Безопасности»
[2]Финансовый университет при Правительстве РФ
[3]НИЯУ МИФИ

23 марта 2023

Коренева А.М., Фирсов Г.В. 23 марта 2023 1 / 24

Коренева А. М., Фирсов Г. В. Характеристики режима работы блочных шифров, предлагаемого для защиты системных носителей информации с блочно-ориентированной структурой. Конференция РусКрипто'2023.

Структура доклада

1. Предварительные сведения
2. Определение схемы TNR
3. Уровень информационной безопасности схемы TNR
4. Сравнение с существующими решениями

Научный фундамент

1. Защищённое хранение данных и полнодисковое шифрование / Е. К. Алексеев, Л. Р. Ахметзянова, А. А. Бабуева, С. В. Смышляев // Прикладная дискретная математика. – 2020. – № 49. – С. 78–97.
2. Минаков С. С. Основные криптографические механизмы защиты данных, передаваемых в облачные сервисы и сети хранения данных // Вопросы кибербезопасности. – 2020. – № 3(37). – С. 66–75.
3. Firsov, G., Koreneva, A. On improved security bounds of one block ciphers mode of operation for protection of block-oriented system storage devices // Journal of Computer Virology and Hacking Techniques. – DOI 10.1007/s11416-024-00528-y.
4. Naor M., Reingold O. On the construction of pseudorandom permutations: Luby-Rackoff revisited // Journal of Cryptology – 1999. – № 1(12). – С. 29-66.

Принятые сокращения

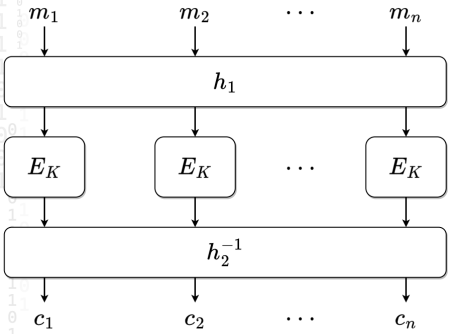
ПДШ (FDE)	—	Полнодисковое шифрование
СБШ	—	Симметричный блочный шифр
CCA	—	Chosen ciphertext attack (атака по подобранному шифртексту)
TNR	—	Схема Tweakable Naor and Reingold
XEH	—	Режим Xor-Encrypt-Hash

Обозначения

$x \xleftarrow{\$} X$	—	равновероятный выбор элемента из конечного мн-ва X
E_K	—	функция зашифрования СБШ на ключе K
D_K	—	функция расшифрования СБШ на ключе K
V_l	—	мн-во двоичных строк длины $l \in \mathbb{N}$
SN	—	номер сектора носителя

Определение схемы TNR

Базовая конструкция



Особенности:

- $h_1 : V_l \to V_l$ и $h_2 : V_l \to V_l$ — обратимые функции;
- для схемы получена оценка уровня ИБ в модели PRP;
- функции h_1 и h_2 являются частью ключа схемы.

Цель текущей работы:

- функции h_1 и h_2 — не часть ключа;
- оценка уровня ИБ в модели RND-fdeCCA-sector.

Naor M., Reingold O. On the construction of pseudorandom permutations: Luby-Rackoff revisited // Journal of Cryptology – 1999. – № 1(12). – С. 29-66.

Firsov, G., Koreneva, A. On improved security bounds of one block ciphers mode of operation for protection of block-oriented system storage devices // Journal of Computer Virology and Hacking Techniques. – DOI 10.1007/s11416-024-00528-y.

Определение схемы TNR

Конструктивные элементы, входные и выходные данные

Конструктивные элементы схемы $TNR^{\mathcal{E}}_{h,\hat{h}}$:

- симметричный блочный шифр $\mathcal{E}$ с длиной блока l и ключевым множеством $\mathcal{K}$;
- биективные по своим последним аргументам функции $h : V_l^s \times V_l^n \to V_l^n$ и $\hat{h} : V_l^r \times V_l^n \to V_l^n$.

Входные данные:

- $k+1$ ключ шифра $\mathcal{E}$, $k \in \mathbb{N}$;
- настройка (номер сектора) SN;
- блоки открытого текста $m_1, ..., m_n$ (шифртекста $c_1, ..., c_n$).

Выходные данные:

- блоки шифртекста $c_1, ..., c_n$ (открытого текста $m_1, ..., m_n$).

Определение схемы TNR

Функции зашифрования и расшифрования

Пусть непустые мн-ва $I = \{i_1, ..., i_s\}$ и $J = \{j_1, ..., j_r\}$ таковы, что:

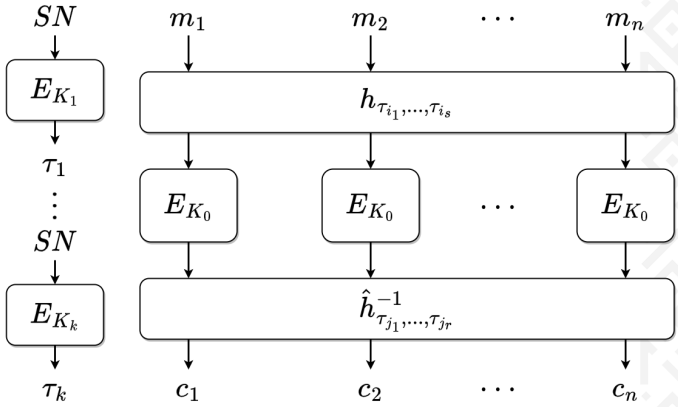
$$I \cup J = \{1, ..., k\}.$$

Обозначим:

$$h_{\tau_{i_1},...,\tau_{i_s}}(\mathbf{x}) = h(\tau_{i_1}, ..., \tau_{i_s}, \mathbf{x}),$$
$$\hat{h}_{\tau_{j_1},...,\tau_{j_r}}(\mathbf{x}) = \hat{h}(\tau_{j_1}, ..., \tau_{j_r}, \mathbf{x}).$$

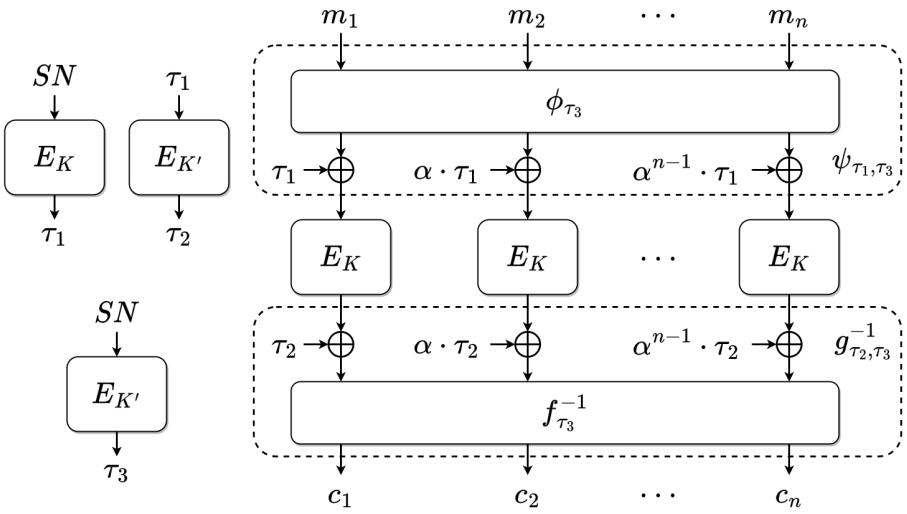
Для каждого $i \in \{1, ..., k\}$:

$$\tau_i = E_{K_i}(SN).$$



Функция зашифрования схемы $TNR^{\mathcal{E}}_{h,\hat{h}}$.

Режим XEH



Режим XEH — вариация схемы TNR

Оценка уровня ИБ схемы TNR

Свойства функций h и $\hat{h}$

Функция $f : \mathcal{K}_f \times X \to Y^n$ называется поблочно почти универсальной с параметрами $\epsilon_1, \epsilon_2, \epsilon_3$ (будем записывать $(\epsilon_1, \epsilon_2, \epsilon_3)$-BAU*), если для любых $x, x' \in X$ и $i, i' \in \{1, ..., n\}$:

при $(i, x) \neq (i', x')$ и $K \xleftarrow{\$} \mathcal{K}_f$:

$$\Pr\left[y_i = y'_{i'}\right] \leq \epsilon_1, i \neq i',$$
$$\Pr\left[y_i = y'_{i'}\right] \leq \epsilon_2, i = i',$$

где $(y_1, ..., y_n) = f(K, x)$,
$(y'_1, ..., y'_n) = f(K, x')$.

при $K \xleftarrow{\$} \mathcal{K}_f$ и $K' \xleftarrow{\$} \mathcal{K}_f$:

$$\Pr\left[y_i = y'_{i'}\right] \leq \epsilon_3,$$

где $(y_1, ..., y_n) = f(K, x)$,
$(y'_1, ..., y'_n) = f(K', x')$.

Для h: $K_h = V_l^s$, $X = Y^n = V_l^n$.
Для $\hat{h}$: $K_{\hat{h}} = V_l^r$, $X = Y^n = V_l^n$.

Оценка уровня ИБ схемы TNR

Вспомогательная схема $TNR^{\pi_0,\dots,\pi_k}_{h,\hat{h}}$: использование подстановок π_i (π_i^{-1}) вместо E_{K_i} (D_{K_i}), $i \in \{0,\dots,k\}$.

Теорема 1 (Уровень ИБ схемы TNR)

Пусть l (длина блока), n (кол-во блоков в секторе), k (количество вспомогательных ключей) — фиксированные натуральные числа.
Пусть $\pi_0,\dots,\pi_k$ — подстановки, выбранные случайно, равновероятно и независимо из $\mathrm{S}(V_l)$.
Если функции h и $\hat{h}$ являются $(\epsilon_1,\epsilon_2,\epsilon_3)$-BAU* и $(\hat{\epsilon}_1,\hat{\epsilon}_2,\hat{\epsilon}_3)$-BAU* соответственно, то:

$$\mathbf{Adv}^{\text{RND-fdeCCA-sector}}_{TNR^{\pi_0,\dots,\pi_k}_{h,\hat{h}}}(q) \le \tilde{\epsilon}_1 \cdot \frac{(2n^2-n)q^2}{4} + \tilde{\epsilon}_2 \cdot \frac{nq^2}{2} + \tilde{\epsilon}_3 \cdot \frac{n^2q^2}{2} + \frac{k}{2} \cdot \frac{q(q-1)}{2^l},$$

где $\tilde{\epsilon_i} = \epsilon_i + \hat{\epsilon_i}$, $i \in \{1,2,3\}$, q — суммарное количество запросов к оракулам в эксперименте RND-fdeCCA-sector.

Сравнение со стандартизированными режимами

Режим	Синхропосылка	Доп. данные	Длина ш.т.	Имитовставка
CBC/CFB	\$	$-$	$>$	$-$
CTR	U	$-$	$>$	$-$
OFB	U/\$	$-$	$>$	$-$
DEC	$-$	$+$	$=$	$-$
MGM	U	$-$	$>$	$+$
CTR-ACPKM	U	$-$	$>$	$-$
TNR/XEH	$-$	$-$	$=$	$-$

Синхропосылка: «\$» — непредсказуемая, «U» — уникальная, «$-$» — не требуется.
Доп. данные: «$-$» — не требуются, «$+$» — требуются.
Длина ш.т.: «$>$» — больше длины о.т., «$=$» — равна длине о.т.
Имитовставка: «$-$» — отсутствует, «$+$» — присутствует.

Область применения

- **Защита информации на системных носителях с блочно-ориентированной структурой, а также на носителях, установленных в ноутбуках**
  Известно не менее 9 отечественных решений с функционалом ПДШ, а также не менее 2 отечественных производителей защищенных носителей информации со встроенным шифрованием.

- **Защита информации в облачных сервисах и сетях хранения данных**

Результаты

- Предложена схема TNR, позволяющая строить режимы работы блочных шифров для защиты информации на системных носителях;
- для схемы TNR получена оценка уровня ИБ, которая может быть использована при выборе параметров конкретных реализаций схемы;
- предложенная схема может быть использована для защиты информации на системных носителях, а также в облачных сервисах и сетях хранения данных.

Спасибо за внимание!

Контактная информация

- Коренева Алиса Михайловна: A.Koreneva@securitycode.ru
- Фирсов Георгий Валентинович: G.Firsov@securitycode.ru